ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΠΟΚΕΝΤΡΩΜΕΝΗ ΔΙΟΙΚΗΣΗ ΚΡΗΤΗΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΣΩΤ. ΛΕΙΤΟΥΡΓΙΑΣ
Δ/ΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ
Πλατεία Κουντουριώτη
712 02 Ηράκλειο
Πληροφορίες.: Παναγιώτης Αργύρης
Τηλ: 2810.278117
e-mail: p.argiris@apdkritis.gov.gr.gr

Ηράκλειο, 22/5/2017
Αριθ.Πρωτ: 418

ΠΡΟΣ: Όλες τις Δ/νσεις

ΘΕΜΑ: ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ στα Συστήματα Πληροφορικής και Επικοινωνιών της Αποκεντρωμένης Διοίκησης Κρήτης

Στην Αποκεντρωμένη Διοίκηση Κρήτης, ακολουθώντας το κρατικό μοντέλο της ηλεκτρονικής διακυβέρνησης (ΗΔ), τις καλές πρακτικές οργανωμένων επιχειρήσεων του ιδιωτικού τομέα αλλά και την ακαδημαϊκή γνώση στην Ασφάλεια Συστημάτων, έχουμε επενδύσει σε υποδομές και πληροφορικά συστήματα τα οποία πρέπει να λειτουργούν αδιάλειπτα και να έχουν επικαιροποιημένη πληροφορία με στόχο την εξυπηρέτηση του πολίτη και τη διαφάνεια. Ειδικότερα, το Τμήμα Σχεδιασμού και Υποστήριξης Συστημάτων πέραν από την προμήθεια και εγκατάσταση σε παραγωγική λειτουργία εξοπλισμού και λογισμικού, ασχολείται με θέματα ασφαλείας και ακεραιότητας δεδομένων ώστε να προβλέψει πιθανά ρίσκα, κενά ασφαλείας και να αποτρέψει μελλοντικά προβλήματα για την υπηρεσία.

Η Ασφάλεια των πληροφοριακών συστημάτων αφορά στη διασφάλιση της ακεραιότητας των δεδομένων, της εμπιστευτικότητας-πρόσβασης σε δεδομένα και της διαθεσιμότητας της πληροφορίας. Η διασφάλιση της ασφάλειας αφορά στα **συστήματα**, στις **διαδικασίες** αλλά και στον **ανθρώπινο παράγοντα** που συμμετέχει στα παραπάνω. Παράλληλα, με τη ραγδαία εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών σήμερα, εξελίσσονται και οι ιοί των Η/Υ. Υπάρχουν ιοί που μπορούν να σβήσουν περιεχόμενο από το σκληρό δίσκο, να κρυπτογραφήσουν αρχεία, να στείλουν πληροφορίες από τον Η/Υ στο διαδίκτυο χωρίς να το αντιληφθεί ο κοινός χρήστης.

Με αφορμή τις πρόσφατες κυβερνοεπιθέσεις σε κυβερνητικά sites (Αριστοτέλειο, Αποκεντρωμένες Διοικήσεις Θεσσαλίας και Μακεδονίας-Θράκης, Νοσοκομεία κ.ά.) και την εξάπλωση σύγχρονων ιών Η/Υ που μεταδίδονται μέσω μηνυμάτων του ηλεκτρονικού ταχυδρομείου (spam-emails), η Δ/νση Πληροφορικής και Επικοινωνιών οφείλει να διασφαλίσει την ασφάλεια των δικτύων και πληροφορικών συστημάτων των υπηρεσιών του φορέα μας με μια σειρά από ενέργειες:

1. Επιβεβαίωση λειτουργίας ενημέρωσης αναβαθμίσεων του λειτουργικού συστήματος των Windows (Updates) για τα Windows 7, 8 και 10 (τα XP δεν υποστηρίζονται πλέον).
2. Επιβεβαίωση λειτουργίας λογισμικού προστασίας από ιούς σε όλους τους Η/Υ.
3. Τείχος προστασίας ενεργό σε μόνιμη βάση στις προεπιλεγμένες ρυθμίσεις.
4. Απεγκατάσταση λογισμικού που μπορεί να προκαλεί διένεξη με άλλα προγράμματα.
5. Εγκατάσταση ειδικής έκδοσης του φυλλομετρητή MozillaFirefox και του JavaRuntime για την ψηφιοποίηση εγγράφων του πρωτοκόλλου.
6. **Διασφάλιση προφίλ διαχειριστή με κωδικό σε κάθε Η/Υ**, ώστε σε περίπτωση δυσλειτουργίας να μπορεί να υπάρχει ελεγχόμενη πρόσβαση και αποκατάσταση του προφίλ και των αρχείων του χρήστη, διασφάλιση ύπαρξης λογισμικού για εξ' αποστάσεως υποστήριξη (teamviewer v.8).
7. Εξασφάλιση διαδικασιών backup στα κεντρικά συστήματα και τους προσωπικούς Η/Υ και εγκατάσταση κεντρικών δίσκων αποθήκευσης (NAS) σε κάθε κτίριο της ΑΠΔΚ.

8. Ισχυρότεροι κωδικοί διαχειριστών στα κεντρικά συστήματα.
9. Προμήθεια και εγκατάσταση ειδικού λογισμικού προστασίας για τους κεντρικούς εξυπηρετητές (Πύλη της Υπηρεσίας, Πρωτόκολλο).
10. Κεντρικά UPS σε όλα τα κεντρικά συστήματα αλλά και Η/Υ που αποθηκεύουν κρίσιμα δεδομένα της υπηρεσίας.

Επιπρόσθετα στα παραπάνω και σε σχέση με τις διαδικασίες και τη συμβολή του ανθρώπινου παράγοντα, είναι επιβεβλημένο να τηρούνται **ορθές πρακτικές** από όλους τους συναδέλφους για την διασφάλιση της πληροφορίας και των συστημάτων στην υπηρεσία μας. Συγκεκριμένα :

1. Προστασία των Η/Υ με σύνθετο κωδικό που περιέχει γράμματα και αριθμούς, κλείδωμα του Η/Υ όταν απομακρυνόμαστε από τη θέση εργασίας μας
2. Πρόσβαση σε κεντρικά συστήματα (πρωτόκολλο, emIS, Διαχείριση Προσωπικού, μισθοδοσία) με τη χρήση των προσωπικών κωδικών μας και διασφάλιση αυτών
3. Διαφύλαξη και αποκλειστική χρήση των ηλεκτρονικών υπογραφών και κλειδιών
4. Οι πληροφορίες της υπηρεσίας, του προσωπικού κ.α. θα πρέπει να καταχωρούνται σε κεντρικά συστήματα εφόσον αυτά είναι διαθέσιμα και να μην τηρούνται σε προσωπικούς Η/Υ (σε μορφή excel, καταλόγων, προσωπικών αρχείων κλπ). Σε περίπτωση βλάβης των σκληρών δίσκων ή επίθεσης από ιό δεν είναι πάντα τεχνικά εφικτό ότι η πληροφορία θα μπορέσει να ανακτηθεί
5. Φύλαξη των κτιρίων και του ηλεκτρονικού εξοπλισμού.
6. Αποφυγή ανοίγματος ύποπτων emails από άγνωστες πηγές, ή emails που έχουν μετακινηθεί αυτόματα στην ανεπιθύμητη αλληλογραφία.
7. Πρόσβαση μόνο σε αξιόπιστες τοποθεσίες στο διαδίκτυο- το Εθνικό Δίκτυο ΣΥΖΕΥΞΙΣ παρέχει ένα βαθμό ασφάλειας.
8. Ηλεκτρονικές πληρωμές σε κατάσταση ασφαλούς πρόσβασης (εμφάνιση **https** στη γραμμή διευθύνσεων του φυλλομετρητή).
9. Ελεγχόμενη φυσική πρόσβαση στα computer-rooms, το τηλεφωνικό κέντρο, τους κεντρικούς εξυπηρετητές και τον ενεργό εξοπλισμό δικτύου.
10. Προσοχή στην αποστολή και προώθηση μαζικών μηνυμάτων.
11. Τακτικό άδειασμα του κάδου ανακύκλωσης του Η/Υ
12. Αποφυγή χρήσης μεγάλων σε μέγεθος ονομάτων αρχείων που περιέχονται σε φακέλους και υποφακέλους με επίσης μεγάλα ονόματα.
13. Φύλαξη φορητών εξωτερικών δίσκων, φορητών υπολογιστών, μονάδων USB και προσωπικών κωδικών σε ασφαλές μέρος.
14. Έλεγχος της ουράς του εκτυπωτή πριν την εκτύπωση εμπιστευτικού υλικού.
15. Καταστροφή των εγγράφων της υπηρεσίας πριν την αποστολή στην ανακύκλωση.
16. Επιστασία στο συνεργείο καθαριότητας ώστε να μην μετακινούνται τα καλώδια των συσκευών.

Επίσης, αφορά συλλογική ευθύνη η ανάπτυξη μιάς κουλτούρας οικονομίας **που αφορά την αποφυγή περιττών εκτυπώσεων**.

Με εντολή Γενικού Γραμματέα
Αποκεντρωμένης Διοίκησης Κρήτης

Κων/νος Στραταριδάκης, PhD
Υπεύθυνος Διεύθυνσης